Operational criterion and constructive checks for the separability of low rank density matrices.

Paweł Horodecki[1,2,*], Maciej Lewenstein[1,**], Guifré Vidal[3***], and Ignacio Cirac[3****]
[1] *Institut für Theoretische Physik, Universität Hannover, D-30167 Hannover, Germany*
[2] *Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80–952 Gdańsk, Poland*
[3] *Institut für Theoretische Physik, Universität of Innsbruck, A-6020 Innsbruck, Austria*

We consider low rank density operators ϱ supported on a $M \times N$ Hilbert space for arbitrary M and N ($M \leq N$) and with a positive partial transpose (PPT) $\varrho^{T_A} \geq 0$. For rank $r(\varrho) \leq N$ we prove that having a PPT is necessary and sufficient for ϱ to be separable; in this case we also provide its minimal decomposition in terms of pure product states. It follows from this result that there is no rank 3 bound entangled states having a PPT. We also present a necessary and sufficient condition for the separability of generic density matrices for which the sum of the ranks of ϱ and ϱ^{T_A} satisfies $r(\varrho) + r(\varrho^{T_A}) \leq 2MN - M - N + 2$. This separability condition has the form of a constructive check, providing thus also a pure product state decomposition for separable states, and it works in those cases where a system of couple polynomial equations has a finite number of solutions, as expected in most cases.

03.67.Hk, 03.65.Bz, 03.67.-a, 89.70.+c

I. INTRODUCTION

Entanglement is one of the quantum properties with no classical counterpart. It is closely connected to fundamental questions of quantum mechanics [1,2], and to physical phenomena which are important for quantum information processing [3]. The relevance of entanglement effects was first demonstrated for pure states. However, in realistic physical situations one deals usually with mixed states, in which pure state entanglement has been significantly weakened by noise. In order to overcome the problems caused by noise (i.e. in order to reduce it) the idea of distillation of entanglement in spatially separated laboratories was introduced [4]. It was proved then [5] that for bipartite systems of low dimensional Hilbert space $\mathcal{C}^M \times \mathcal{C}^N$ or simply $M \times N$ (namely systems with $M = 2$ and $N = 2$ or 3) mixed state entanglement can always be distilled into its pure form. However, it turned out that in higher dimensional systems ($MN > 6$) bound entanglement [6] – which cannot be distilled, as opposed to free entanglement – exists.

Unlike in the case of pure states, it is in general very difficult to know whether a given mixed state is entangled (inseparable) or non-entangled (separable). According to the definition a state supported on a Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ is separable if and only if it can be written in (or approximated by) the form [7]

$$\varrho = \sum_{i=1}^{k} p_i |e_i, f_i\rangle\langle e_i, f_i|, \quad \sum_i p_i = 1, \tag{1}$$

where $|e_i, f_i\rangle$ stands here for a normalized vector $|e_i\rangle \otimes |f_i\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. In finite dimensional cases, the ones we will be concerned here, the approximation part is not necessary, as for any separable state one can always find a set $\{|e_i, f_i\rangle\}$ of product vectors for which $k \leq \dim(\mathcal{H}_{AB})^2$ in the above formula [8].

Several necessary conditions for separability are known: Werner derived a condition based on the analysis of local hidden variables models and mean value of the, so called, flipping operator [7]; the Horodeckis proposed a necessary criterion based on α-entropy inequalities [9]. Peres demonstrated that the partial transpose ϱ^{T_A} of the matrix ϱ, defined as $\langle m, \mu|\varrho^{T_A}|n, \nu\rangle = \langle n, \mu|\varrho|m, \nu\rangle$ for any fixed product basis $|n, \nu\rangle \equiv |e_n\rangle_A \otimes |e_\nu\rangle_B$, must be still a legitimate density matrix if ϱ is separable [10]. This operationally friendly, necessary condition, called positive partial transpose (PPT) condition, turned out to be very strong.

Soon after Peres result, a general connection between positive map theory and separability was established in [11], where necessary and sufficient separability conditions were derived in terms of positive maps. In particular it implied that for systems of low dimensions ($MN \leq 6$) the PPT condition is also sufficient for separability. It was also shown that this is not the case for systems of higher dimensions ($MN > 6$). Later on explicit counterexamples of entangled states with PPT property were provided by means of another separability criterion, based on the analysis of the range of the density matrix [8] (cf. [12]). It was then shown that they represent bound entanglement [6]. Let us note that on mathematical grounds there were examples, provided earlier [13], of elements of positive matrices cones which can be treated as prototypes of PPT entangled states.

Sufficient conditions for separability are also known. We remark that the results of [14] readily imply that any state close enough to the completely random state π is separable. Thus, as quantified in [15], any mixture $\tilde{\varrho} = (1-p)\varrho + p\pi$ in a $M \times N$ system is separable if $p \geq (1 + 2/MN)^{-1}$ or, in other words, as we wish to make explicit here, a full rank mixed state is separable provided its smallest eigenvalue be greater than or equal to $(2 + MN)^{-1}$.

On the other hand the analysis of the range of the den-

sity matrices, first applied in the separability criterion [8], led to an algorithm for the optimal decomposition of mixed states into a separable and an inseparable part [16], and to a systematic method of constructing examples of PPT entangled states and peculiar positive maps [17,18]. Also, the technique of diminishing the rank of a PPT density matrix by subtraction of selected product vectors, which was worked out in [19], turned out to be very useful. This and other techniques have allowed quite recently to study operational necessary and sufficient separability conditions for states of a $2 \times N$ system [20]. In particular it has been shown that:

(i) all PPT states of rank smaller than N are separable;

(ii) the separability of generic states such that $r(\varrho) + r(\varrho^{T_A}) \leq 3N$ reduces to analyzing the roots of some complex polynomials (a constructive separability criterion was derived, thus providing also the decomposition of such separable states into pure product states);

(iii) states invariant under partial transpose, and those that are not "very different" from their partial transpose are necessarily separable.

This paper can be considered an extension and generalization of Ref. [20]. The results (i) and (ii) obtained there for $2 \times N$ systems are here generalized non-trivially to the case of $M \times N$ systems ($M \leq N$). We show, namely, that

- any state ϱ supported on $M \times N$ ($M \leq N$) and with rank $r(\varrho) \leq N$ is separable iff its partial transpose is positive;
- separability of generic PPT density matrices with $r(\varrho) + r(\varrho^{T_A}) \leq 2MN - M - N + 2$ reduces to solving a system of coupled polynomial equations.

In both cases a pure product state decomposition for separable states is obtained.

Throughout this paper we make use of the following definition: we say that a state ρ acting on $M \times N$ is *supported* on $M \times N$ if this is the smallest product Hilbert space on which ρ can act. Let us introduce the local ranks $r(\varrho_A)$ and $r(\varrho_B)$, where $\varrho_{A,B} \equiv \mathrm{Tr}_{A,B}\varrho$ are the reduced density operators. It immediately follows from the first of the above results that there is no PPT bound entanglement of rank 3. Indeed, a rank 3 state ρ either has at least one of the local ranks $r(\rho_A)$ and $r(\rho_B)$ greater than 3, and in this case is distillable [26] (i.e., ρ^{T_A} is not positive), or else can be supported on a $MN \leq 6$ or on a 3×3 system, and thus is separable. This implies in particular that the bound entangled states constructed with the UPB method [17] and those based on the chess-board structure of eigenvectors [21] are *optimal* with respect to their ranks.

For our second main result, concerned with those PPT density matrices for which the sum of ranks satisfies $r(\varrho) + r(\varrho^{T_A}) \leq 2MN - M - N + 2$, we identify the eligible product vectors (that is, those that can appear in decomposition (1) if ρ is separable) with the solutions of a system of coupled polynomial equations. We analyze these equations, which are arguably expected to have only a finite number of solutions. For this case we present a constructive (i.e. leading to a product state decomposition) method to check separability. Also for the same case we discuss an alternative, constructive method to check separability numerically. These checks represent a necessary and sufficient condition for separability.

We wish to remark the importance of having separability conditions for low rank density matrices, especially in relation to unsolved problems concerning the nature of bound entanglement (BE). Notice that such conditions are of great value when trying to construct states with BE. Among the open questions we encounter the existence of BE having a non-positive partial transpose NPT (see [22]). Also, whether a finite or a vanishing amount of free entanglement is required to asymptotically create bound entangled states. There are in addition several conjectures concerning bound entanglement (see [6,17,23–25]) among them the ones connected to capacities of quantum channels and bound entanglement assisted distillation. Finally, we have been recently able to establish a general connection between low rank bound entangled states and positive maps. This connection allows for a systematic construction of independent linear maps in arbitrary dimensions, including $2 \times N$, where the procedures based on unextendible product bases do not work [18]. The discussion of this connection will be presented elsewhere.

This paper is organized as follows: we start by generalizing some needed results of [20] related to diminishing the rank of ρ by subtracting projectors on product vectors; in Section III we present our theorem about the separability of states with rank $\leq N$; in Section IV the necessary and sufficient separability conditions for generic matrices with $r(\varrho) + r(\varrho^{T_A}) \leq 2MN - M - N + 2$ are formulated, and discussed in the context of 3×3 systems; finally, Section V contains our conclusions and acknowledgments.

II. DIMINISHING OF THE RANK - GENERALIZATIONS

Before we turn to the main results of this paper we need to generalize some of those presented in [20].

Consider a state ϱ of a $M \times N$ system satisfying $\varrho^{T_A} \geq 0$. Throughout this paper $K(X), R(X), k(X)$, and $r(X)$ denote the kernel, the range, the dimension of the kernel, and the rank of the operator X, respectively. By $\{|a_i\rangle\}_{i=1}^{M}$ and $\{|b_i\rangle\}_{i=1}^{N}$ we will denote orthonormal basis in $\mathcal{H}_A$ and $\mathcal{H}_B$, and by $|e^*\rangle$ we will denote the complex conjugated vector of $|e\rangle$ in the orthonormal basis $|1\rangle_A, \cdots, |M\rangle_A$ in which we perform the partial transposition; that is, if $|e\rangle = \sum_{i=1}^{M} \alpha_i |i\rangle$ then $|e^*\rangle = \sum_{i=1}^{M} \alpha_i^* |i\rangle$.

For the time being we do not require $M \leq N$. The following Lemma is a generalization of Lemma 6 of Ref. [20] proved there for $M = 2$:

Lemma 1.- If $\exists\ |f\rangle \in \mathcal{C}^N$ such that $|a_i, f\rangle \in K(\varrho)$ for $i = 1, ..., M-1$, then either (i) $|a_M, f\rangle \in K(\varrho)$ or (ii)

$$\begin{aligned} \varrho|a_M, f\rangle &= |a_M, g\rangle \\ \varrho^{T_A}|a_M{}^*, f\rangle &= |a_M{}^*, g\rangle \end{aligned} \tag{2}$$

for some $|g\rangle \in \mathcal{C}^N$.

Proof.- From the assumptions we have immediately $\varrho^{T_A}|a_i{}^*, f\rangle = 0$ $(i = 1, ..., M-1)$. In particular $\forall |h\rangle \in \mathcal{C}^N$ we have $\langle a_M{}^*, h|\varrho^{T_A}|a_i{}^*, f\rangle = 0$ or, equivalently, $\langle a_i, h|\varrho|a_M, f\rangle = 0$. Since $|h\rangle$ is arbitrary we have either statement (i) or $\varrho|a_M, f\rangle = |a_M, g\rangle$ for some $|g\rangle \neq 0$. The second case needs further analysis. In a similar way we can prove that either $\varrho^{T_A}|a_M{}^*, f\rangle = 0$ (which is still equivalent to the statement (i)) or $\varrho^{T_A}|a_M{}^*, f\rangle = |a_M{}^*, g'\rangle$ for some $|g'\rangle \neq 0$. It remains to prove that $|g'\rangle = |g\rangle$. Indeed $|g'\rangle = \langle a_M{}^*|\varrho^{T_A}|a_M{}^*, f\rangle = \langle a_M|\varrho|a_M, f\rangle = |g\rangle$.

The second lemma below is also a generalization of the results from Ref. [20]:

Lemma 2.- If ϱ satisfies the assumptions of Lemma 1, and the possibility (ii) of Lemma 1 holds, then

$$\varrho_1 = \varrho - \lambda |a_M, g\rangle\langle a_M, g|, \tag{3}$$

where $\lambda \equiv \langle a_M, g|\varrho^{-1}|a_M, g\rangle$ and

(i) ϱ_1 is a PPT state with $r(\varrho_1) = r(\varrho) - 1$ and $r(\varrho_1^{T_A}) = r(\varrho^{T_A}) - 1$.

(ii) ϱ_1 is supported either on a $(M-1)\times(N-1)$ or on a $M \times (N-1)$.

(iii) ϱ_1 is separable iff ϱ is separable.

Proof .- Following Corollary 1 and Lemma 2 from Ref. [20], we observe that

$$\varrho_1 = \varrho - \frac{|a_M, g\rangle\langle a_M, g|}{\langle a_M, g|\varrho^{-1}|a_M, g\rangle} \tag{4}$$

is positive, and that $r(\varrho_1) = r(\varrho) - 1$. Then (i) follows from taking into account that since

$$\begin{aligned} \lambda^{-1} &= \langle a_M, g|\varrho^{-1}|a_M, g\rangle = \\ \langle g|f\rangle &= \langle a_M{}^*, g|\varrho^{T_A\,-1}|a_M{}^*, g\rangle, \end{aligned} \tag{5}$$

we have that

$$\varrho_1{}^{T_A} = \varrho^{T_A} - \frac{|a_M{}^*, g\rangle\langle a_M{}^*, g|}{\langle a_M{}^*, g|\varrho^{T_A\,-1}|a_M{}^*, g\rangle}, \tag{6}$$

so that also $\varrho_1^{T_A}$ is positive and $r(\varrho_1^{T_A}) = r(\varrho^{T_A}) - 1$. From assumptions on the kernel of ϱ it follows that all vectors $\{|a_i, f\rangle\}_{i=1}^M$ belong to the kernel of ϱ_1, hence ϱ_1 can be embedded into a $M \times (N-1)$ space; on the other hand since $\varrho_{1,A} = \varrho_A - \lambda\langle g|g\rangle|a_M\rangle\langle a_M|$, $r(\varrho_{1,A})$ must be either $M = r(\varrho_A)$ or $M-1$, which finishes the proof of (ii). In order to prove (iii) let us assume that ϱ is separable and let us show that also ϱ_1 is so (if ϱ_1 is separable then obviously ϱ is also separable). Since $\varrho|a_i, f\rangle = 0$ $(i = 1, ..., M-1)$, we can always write

$$\varrho = \sum |e_i, f_i\rangle\langle e_i, f_i| + |a_M\rangle\langle a_M| \otimes \eta, \tag{7}$$

where $\langle f|f_i\rangle = 0$ and η is a positive operator acting on $\mathcal{C}^N$. If we impose $|a_M, g\rangle = \varrho|a_M, f\rangle$ we obtain $|g\rangle = \eta|f\rangle$, and therefore $|g\rangle \in R(\eta)$. We can write

$$\varrho_1 = \sum |e_i, f_i\rangle\langle e_i, f_i| + |a_M\rangle\langle a_M| \otimes (\eta - \lambda|g\rangle\langle g|), \tag{8}$$

so that if we show that the operator $(\eta - \lambda|g\rangle\langle g|) \geq 0$ then we have that ρ_1 is separable. Using (5) we have that such an operator is

$$\eta - \frac{1}{\langle g|f\rangle}|g\rangle\langle g| = \eta - \frac{1}{\langle g|\eta^{-1}|g\rangle}|g\rangle\langle g|, \tag{9}$$

and that therefore it is positive (cf. Lemma 1 in [20]). □

III. ALL RANK N PPT STATES SUPPORTED ON A $M \times N$ SYSTEM ($M \leq N$) ARE SEPARABLE

In this section we generalize the following theorem proved in Ref. [20]:

Theorem.-[Theorem 1 of Ref. [20]]

Let ϱ be a PPT state of rank N supported on a $2 \times N$ space. Then ϱ is separable and can be written as

$$\varrho = \sum_{i=1}^{N} |e_i, f_i\rangle\langle e_i, f_i| \tag{10}$$

with all $\{|f_i\rangle\}$ linearly independent.

We will express a density matrix in terms of its reduced operators $\langle i_A|\varrho|j_A\rangle$ acting on $\mathcal{H}_B$. For instance, we will write (10) as

$$\varrho = \begin{bmatrix} \tilde{A} & \tilde{B}^\dagger \\ \tilde{B} & \tilde{C} \end{bmatrix}, \tag{11}$$

where $\tilde{A} \equiv \langle 1|\rho|1\rangle \geq 0$, $\tilde{C} \equiv \langle 2|\rho|2\rangle \geq 0$ and $\tilde{B} \equiv \langle 2|\rho|1\rangle$. More generally, a $M \times N$ density matrix will be expressed as

$$\varrho = \begin{bmatrix} E_{11} & E_{12} & ... & E_{1M} \\ E_{12}^\dagger & E_{22} & ... & ... \\ ... & ... & ... & ... \\ E_{1M}^\dagger & ... & ... & E_{MM} \end{bmatrix}, \tag{12}$$

where now $E_{ij} \equiv \langle i_A|\varrho|j_A\rangle$. We start by using the previous Theorem to prove:

Lemma 3.- Let ϱ be a rank N PPT state supported on a $2 \times N$ space. Then after a reversible local filtering operation [1] the state is proportional to the matrix (called hereafter $2 \times N$ *canonical form*):

$$\Sigma \equiv \begin{bmatrix} B^\dagger B & B^\dagger \\ B & I \end{bmatrix} = [B \;\; I]^\dagger [B \;\; I], \tag{13}$$

with B normal, i.e. $[B, B^\dagger] = 0$.

Proof .- We write the density matrix (10) in the form (11). Because there is only a finite number of $|e_i\rangle$ in (10) we can always find a vector $|a\rangle$ such that $\langle a|e_i\rangle \neq 0$ for all i. Let this $|a\rangle$ be the second element of the orthonormal basis in Alice's space, i.e. $|2\rangle = |a\rangle$. The matrix

$$\tilde{C} = \langle a|\varrho|a\rangle = \sum_{i=1}^{N} |\langle a|e_i\rangle|^2 |f_i\rangle\langle f_i|$$

has then maximal rank N, since the $|f_i\rangle$ are linearly independent. Taking the local filter $V = (\sqrt{\tilde{C}})^{-1}$ on Bob's side (this corresponds to sandwitching the state between $I \otimes V$ and $I \otimes V^\dagger$) we obtain

$$\tilde{\varrho} = \begin{bmatrix} A & B^\dagger \\ B & I \end{bmatrix}, \tag{14}$$

which is still positive and PPT (because any local operation preserves the PPT property [6]). We can write

$$\tilde{\varrho} = \Sigma + \mathrm{diag}[\Delta, 0], \tag{15}$$

where the positive matrix Σ from the expression (13) has rank $r(\Sigma) = N$ as its kernel $K(\Sigma)$ has at least dimension N containing all vectors of the type

$$|\phi_f\rangle = |1\rangle|f\rangle + |2\rangle|-Bf\rangle, \tag{16}$$

while its range has at least dimension N due to the identity entry on the diagonal. Notice that $\mathrm{diag}[\Delta, 0]$ is also positive, because positivity of $\tilde{\varrho}$ implies that $\Delta = A - B^\dagger B \geq 0$ [27]. Now, since in addition $r(\tilde{\rho}) = r(\Sigma)$, we also have that $R(\tilde{\rho}) = R(\Sigma) \supseteq R(\mathrm{diag}[\Delta, 0])$, that is $K(\mathrm{diag}[\Delta, 0]) \supseteq K(\Sigma)$. But $K(\Sigma)$ is spanned by the states (16), for which then $\langle\phi_f|\mathrm{diag}[\Delta, 0]|\phi_f\rangle = 0$, which finally implies $\Delta|f\rangle = 0 \;\; \forall |f\rangle$. This ends the proof of the fact that $\Delta = 0$, or in another words that $A = B^\dagger B$. This proves therefore the canonical form (13), but not yet the normality of B. The latter property can be simply proven from the positivity of $\tilde{\varrho}^{T_A}$, which implies that $BB^\dagger - B^\dagger B \geq 0$ [27]. The latter (positive) operator has at the same time null trace and therefore it must vanish. Thus B is normal as stated.□

Let us prove now the generalization of Lemma 3 to the case of $3 \times N$ systems ($N \geq 3$), and then to the $M \times N$ case, where $M \leq N$ from now on.

Lemma 4.- Let ϱ be a PPT state of rank N in a $3 \times N$ space. Let the reduced state ϱ_B and the entry E_{33} in some local basis have also the same rank N. Then ϱ can be transformed using some reversible local transformation to the canonical form:

$$\varrho \sim [C, B, I]^\dagger [C, B, I] \tag{17}$$

where C, B are normal and $[B, C^\dagger] = [B, C] = 0$.

Note that in Lemma 4, in contrast to Lemma 3, we assume that in some basis $r(E_{33}) = N$. Later on, in Theorem 1, we will prove that this assumption is always satisfied.

Proof .- In order to obtain the identity matrix I at the diagonal we use an analogous reversible local filter to the one used in the proof of Lemma 3. After that we readily obtain the form

$$\varrho \sim \tilde{\varrho} = \begin{bmatrix} C^\dagger C & D^\dagger & C^\dagger \\ D & B^\dagger B & B^\dagger \\ C & B & I \end{bmatrix}. \tag{18}$$

with both B and C normal and some unknown D. Indeed, expression (18) as well as the normality of B and C follow from the fact that after a local projection by projectors $P_k \otimes I \equiv (|k\rangle\langle k| + |3\rangle\langle 3|) \otimes I$, $k = 1, 2$ we get a $2 \times N$ state satisfying the assumptions of Lemma 3.

Now, notice that $\langle\Psi_f|\tilde{\varrho}|\Psi_f\rangle = 0$ for $|\Psi_f\rangle \equiv |2\rangle|f\rangle - |3\rangle|Bf\rangle$. Since $\tilde{\varrho} \geq 0$ we have that

$$0 = \tilde{\varrho}|\Psi_f\rangle = |1\rangle|D^\dagger f - C^\dagger B f\rangle, \tag{19}$$

which, as f is arbitrary, leads to $D^\dagger = C^\dagger B$. Thus formula (17) holds. Finally e shall use the latter as well as normality of B and C to prove that $[B, C^\dagger] = [B, C] = 0$. We have

$$\varrho^{T_A} \sim \tilde{\varrho}^{T_A} = \begin{bmatrix} C^\dagger C & B^\dagger C & C \\ C^\dagger B & B^\dagger B & B \\ C^\dagger & B^\dagger & I \end{bmatrix}, \tag{20}$$

and we can check that for any $|f\rangle \in \mathcal{C}^N$ and for $|\Phi_f\rangle \equiv |2\rangle|f\rangle - |3\rangle|B^\dagger f\rangle$, $\langle\Phi_f|\tilde{\varrho}^{T_A}|\Phi_f\rangle = 0$. As ϱ is PPT this implies that

$$\varrho^{T_A}|\Phi_f\rangle = |1\rangle|[B^\dagger, C]f\rangle \tag{21}$$

must vanish. Since the above equation holds for arbitrary $|f\rangle$ we have immediately that $[B, C^\dagger] = [C, B^\dagger]^\dagger = 0$ Normality of B and of $C^\dagger$ implies that these operators can be decomposed as a complex linear combination of projectors into eigenvectors. That they commute means that they actually have the same eigenvectors, and thus so do B and C, i.e. $[B, C] = 0$.□

[1] A reversible transformation is a transformation that can be reversed with nonzero probability. A local filtering in Bob's side $I \otimes V$ is then reversible iff the operator V can be inverted, i.e. iff V^{-1} exists.

Lemma 5.- Any PPT state supported on a $M \times N$ space ($M \leq N$) satisfying that (i) $r(\varrho) = N$, (ii) in some product basis $r(E_{ii}) = N$ for some i, can be transformed after a reversible local transformation to the canonical form:

$$\varrho \sim Z^\dagger Z = [C_1, ..., C_{M-1}, I]^\dagger [C_1, ..., C_{M-1}, I] \qquad (22)$$

with $[C_i, C_j^\dagger] = [C_i, C_j] = 0$, $i, j = 1, ..., M-1$.

Proof .- It follows easily from the application of Lemmas 3 and 4. In particular one has to use the local projections $P \otimes I = (|k\rangle\langle k| + |M\rangle\langle M|) \otimes I$, $1 \leq k < M$, $P' \otimes I = (|m\rangle\langle m| + |m'\rangle\langle m'| + |M\rangle\langle M|) \otimes I$, $1 \leq m < m' < M$.□

As an immediate consequence we have

Lemma 6 .- Any PPT state supported on a $M \times N$ space ($M \leq N$) satisfying that (i) $r(\varrho) = N$, (ii) in some product basis $r(E_{ii}) = N$ for some i, is separable and can be expressed as

$$\tilde{\varrho} = \sum_{i=1}^{N} |e_i, f_i\rangle\langle e_i, f_i|, \qquad (23)$$

where the $\{|e_i\rangle\}$ are possibly unnormalized and the $\{|b_i\rangle\}$ are linearly independent.

Proof .- We make use of Lemma 5. It is easy to see that the matrix $Z^\dagger Z$ has nonzero eigenvectors of the form $|a_i, b_i\rangle$. Here $|b_i\rangle$ is the $i-$th common eigenvector of all operators C_j, $C_k^\dagger$ while $|e_i\rangle^\dagger = [c_i^{(1)}, ..., c_i^{(M-1)}, 1]$ is a row of all $i-$th eigenvalues of matrices $C_1, ..., C_{M-1}, I$. Thus, after some reversible local transformation the state ρ becomes:

$$\tilde{\varrho} = \sum_{i=1}^{N} |e_i, b_i\rangle\langle e_i, b_i|, \qquad (24)$$

where the $\{|b_i\rangle\}$ are orthonormal. Reversing the previous local filtering we obtain (23) □.

Remark .- The above procedure gives a constructive algorithm to decompose any state which satisfies the assumptions of the Lemma.

The main disadvantage of the above results is that all of them contain assumptions about $r(E_{ii}) = N$ for some i and for some product basis, which as we have mentioned, are not necessary. Our main theorem is free of that assumption (i.e., it shows that such E_{ii} always exists). To prove it we have to use induction with respect to $M + N = K$ and use the previous Lemmas. We consider only $r(\varrho) = N$, as a PPT state supported on $M \times N$ cannot have smaller rank. Indeed, since $r(\varrho_B) = N$, if $r(\varrho) < N$ then ϱ is distillable, which implies that ϱ^{T_A} is not positive [26].

Theorem 1.- All rank N PPT states ϱ supported on $M \times N$ are separable.

Proof.- We will prove that in some product basis we have $r(E_{ii}) = N$ for some i. Separability of ϱ will follow from the previous Lemmas. Let us observe that the Theorem and the latter fact are true for $M = 2$ and arbitrary $N \geq 2$. In particular they are true for $M + N = K = 4$ and 5. Let us assume that they hold for $M + N \leq K$. We shall now demonstrate that they also hold for $M + N = K + 1$.

To this aim let us consider the case of ϱ supported on a $(M+1) \times N$ space, with $M + 1 \leq N$, $r(\varrho_A) = M + 1$, $r(\varrho_B) = N$. and $M + N = K$. In an orthonormal, product basis representation the state ϱ has the form of a $(M+1) \times (M+1)$ matrix with $N \times N$ entries

$$\varrho = \begin{bmatrix} E_{11} & E_{12} & ... & E_{1,M+1} \\ E_{12}^\dagger & E_{22} & ... & ... \\ ... & ... & ... & ... \\ E_{1,M+1}^\dagger & ... & ... & E_{M+1,M+1} \end{bmatrix}. \qquad (25)$$

Let us consider the following $M \times M$ submatrix of ϱ

$$W(\varrho) \equiv W = \begin{bmatrix} E_{22} & E_{23} & ... & E_{2,M+1} \\ E_{23}^\dagger & E_{22} & ... & ... \\ ... & ... & ... & ... \\ E_{2,M+1}^\dagger & ... & ... & E_{M+1,M+1} \end{bmatrix}, \qquad (26)$$

resulting after removing the first row and the first column from the representation (25). As the latter action can be achieved by a local projection on Alice's side, W is an unnormalized PPT state acting in $M \times N$. For Bob's reduced matrix $W_B = Tr_B(W)$, we shall consider two alternative possibilities: (i) $r(W_B) = N$, (ii) $r(W_B) < N$.

In case (i) we must have $r(W) = N$ as otherwise we would have that the global rank is less than one of the local ranks, resulting in distillability of ϱ, *ergo* in violation of the PPT condition [6,26]. But it means that W is a PPT state supported on $M \times N$ with global and local rank equal to N. According to the induction assumption, it is thus separable and for some product basis has an entry E_{ii} for some $i = 2, \ldots, M+1$ with the rank N. But then ϱ has an entry E_{ii} with rank N in the same product basis, and from Lemmas 5 and 6 it follows immediately that it is separable.

Consider now case (ii). If W has $r(W_B) < N$, then obviously there exist a sequence of product vectors $|a_i, f\rangle \in K(W)$, $i = 2, ..., M+1$. It is immediate to check that they must belong to kernel of ϱ. That means that the assumptions of the Lemma 1 are fulfilled. The possibility (i) of this Lemma cannot hold because otherwise one could embed ϱ into $(M+1) \times (N-1)$ space, and $r(\varrho_B)$ would be $N-1$ instead of N. The possibility (ii) of Lemma 1 means that ϱ can be written in the form (cf. Lemma 2)

$$\varrho = \varrho' + \lambda |1, g\rangle\langle 1, g| \qquad (27)$$

where ϱ' is a rank $N-1$ PPT state supported either on a $(M+1) \times (N-1)$ subspace or on a $M \times (N-1)$ subspace, $\lambda^{-1} \equiv \langle 1, g|\rho^{-1}|1, g\rangle$ and $|1, g\rangle\langle 1, g|$ is an

unnormalized projector onto a product state such that $\varrho^{-1}|1,g\rangle$ is orthogonal to $R(\varrho')$.

At the same time it must hold that $r(\varrho'_B) = N-1$, since i) Bob's space has now only $N-1$ dimensions, ii) $r(\varrho'_B)$ cannot be smaller than $N-1$, since $N = r(\varrho_B = \varrho'_B + |g\rangle\langle g|)$ and $|g\rangle\langle g|$ can increase at most in one unit the rank of ϱ'_B. All that means that the matrix ϱ' fulfills the induction assumption as $(M+1)+(N-1) = K$ (or $M+(N-1) = K-1$) and $r(\varrho') = r(\varrho'_B)$, *ergo* it is separable and has in some product basis $|a_i, b_j\rangle$ the entry $E'_{ii} = \langle a_i|\varrho'|a_i\rangle$ with rank $N-1$. Lemma 6 implies then that ϱ $(= \varrho' + \lambda|1,g\rangle\langle 1,g|)$ can be decomposed into

$$\sum_{i=1}^{N-1} |e_i, f_i\rangle\langle e_i, f_i| + \lambda|1,g\rangle\langle 1,g|, \tag{28}$$

where $|g\rangle$ is linearly independent from the set of (also linearly independent) vectors $|b_i\rangle$. Since there is only a finite number of projectors in the decomposition above, we can always find a vector $|a\rangle$ in Alice's space such that $\langle e_i|a\rangle \neq 0 \neq \langle 1|e\rangle$. Including such a vector in a product basis to express ϱ we will obtain the wished rank N element $\langle a|\varrho|a\rangle$. This completes the proof of the induction step, and by induction completes thus the proof of the theorem. □

IV. SEPARABILITY CRITERIA FOR RANK(ϱ)+RANK(ϱ^{T_A}) $\leq 2MN - M - N + 2$

In this section we generalize the results obtained for $2 \times N$ systems in Ref. [20]. The idea is that a PPT density operator ϱ with $r(\varrho) + r(\varrho^{T_A}) \leq 2MN - M - N + 2$ may have a finite number of product vectors $|e_i, f_i\rangle$ in its range, such that $|e_i^*, f_i\rangle \in R(\varrho^{T_A})$. These product vectors are the only possible candidates to appear in decomposition (1) [8]. Finding them requires solving a system of polynomial equations. First we show how to solve these equations in a *generic* case (namely when the coefficients of such equations do not happen to satisfy a large series of conditions, which amounts to having only a finite number of solutions), and once all the product states $\{|e_i, f_i\rangle\}_{i=0}^{L<\infty}$ have been obtained, we present an algorithmic method to check whether ρ is separable. This is done in a finite number of computational steps, and thus solves operationally the problem of separability for states with $r(\varrho) + r(\varrho^{T_A}) \leq 2MN - M - N + 2$ and finite L.

A. Eligible product vectors.

Let the linearly independent vectors $|K_i\rangle$, $|\tilde{K}_i\rangle$ form a basis in the kernel of ϱ and in the kernel of ϱ^{T_A}, respectively:

$$K(\varrho) = \text{span}\{|K_i\rangle, i = 1, ..., k(\varrho)\} \tag{29}$$

$$K(\varrho^{T_A}) = \text{span}\{|\tilde{K}_i\rangle, i = 1, ..., k(\varrho^{T_A})\} \tag{30}$$

We consider here the case when $k(\varrho) + k(\varrho^{T_A}) \geq M + N - 2$. We can always expand $|K_i\rangle$ and $|\tilde{K}_i\rangle$ in an orthonormal basis in Alice's space

$$|K_i\rangle = \sum_{m=0}^{M} |m, k_i^m\rangle, \tag{31}$$

$$|\tilde{K}_i\rangle = \sum_{m=0}^{M} |m, \tilde{k}_i^m\rangle. \tag{32}$$

A product vector $|e, f\rangle$ belonging to the range $R(\varrho)$ must be orthogonal to all $|K_i\rangle$; simultaneously, if its partial complex conjugation belongs to $R(\varrho^{T_A})$, $|e^*, f\rangle$ must be orthogonal to all $|\tilde{K}_i\rangle$. Thus the eligible product vectors are the solutions of $k(\varrho) + k(\varrho^{T_A})$ equations, namely

$$\begin{aligned} &\langle K_i|e, f\rangle = 0, i = 1, ..., k(\varrho), \\ &\langle \tilde{K}_i|e^*, f\rangle = 0, \ i = 1, ..., k(\varrho^{T_A}). \end{aligned} \tag{33}$$

Let us now expand $|e\rangle$ in the above formula as:

$$|e\rangle = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_M \end{bmatrix}. \tag{34}$$

We restrict ourselves to $\alpha_1 = 1$. The reason is that we expect to find only a *finite* number L of inequivalent vectors $|e_i, f_i\rangle$ that fulfill the requirements. A generic choice of an orthonormal basis $\{|a_i\rangle\}$ in Alice's space will imply that $\langle 1|a_i\rangle \neq 0$ for all $i = 1, \ldots, L$. In this basis α_1 can be set equal to 1.

Equations (33) can be rewritten as follows:

$$A(\alpha_1, ..., \alpha_M; \alpha_1^*, ..., \alpha_M^*)|f\rangle = 0, \tag{35}$$

where the $[k(\varrho) + k(\varrho^{T_B})] \times N$ matrix A is defined as follows:

$$\begin{aligned} A(\alpha_1, ..., \alpha_M; \alpha_1^*, ..., \alpha_M^*) &\equiv \begin{bmatrix} \sum_{m=1}^M \alpha_m \langle k_1^m| \\ ... \\ \sum_{i=1}^M \alpha_m \langle k_{k(\varrho)}^m| \\ \sum_{i=1}^M \alpha_m^* \langle \tilde{k}_1^m| \\ ... \\ \sum_{i=1}^M \alpha_m^* \langle \tilde{k}_{k(\varrho^{T_A})}^m| \end{bmatrix} \\ &\equiv \begin{bmatrix} D_{k(\varrho)\times N}(\alpha) \\ \tilde{D}_{k(\varrho^{T_B})\times N}(\alpha^*) \end{bmatrix}. \end{aligned} \tag{36}$$

If (35) holds for some $|f\rangle \neq 0$ and $|e\rangle \neq 0$, this means that for the corresponding set of α's the rank of A is smaller than N. Therefore, in order to identify eligible product vectors we have to require that at most $N-1$ rows of A be linearly independent vectors. In what follows we restrict ourselves to the limiting case

$k(\varrho) + k(\varrho^{T_A}) = M + N - 2$, the others containing more restrictions and consequently less solutions than this.

Let us then take $N-1$ rows of A, say the first ones, and let us require that each of the remaining $M-1$ rows be linearly dependent of them. Recall that we can use the $M-1$ variables $\alpha_2, \cdots, \alpha_M$ in order to achieve this. Then, parameter counting strongly suggests that we need to fix all the $M-1$ α's in order to make A have rank smaller than N, this corresponding to a zero measure set of points in the α-space $[\alpha_1{=}1, \alpha_2, \cdots, \alpha_M]$. We will in addition relate the number of solutions to the roots of complex polynomials, which under *generic* conditions have only a finite number of roots. Numerical experience acquired for the $2 \times N$ case further supports the expectation that the number of solutions *be* typically finite.

B. Generic Polynomials.

Let us discuss a bit further sufficient conditions for the existence of a finite set of solutions, while presenting a systematic method to find them once the conditions are fulfilled. This method also works for $k(\varrho) + k(\varrho^{T_A}) < M + N - 2$ by just adding more equations.

Matrix A will have at most rank $N-1$ after requiring that all its rank N minors vanish. At risk of finally finding more solutions than just those of equations (35), we can impose that only $M-1$ of these minors vanish. The reason for doing so is that this will already allow us to prove that only a finite number of product vectors fulfill (33) under some *generic* circumstances. Thus we consider the determinant of $N \times N$ submatrices of A formed by taking its first $N-1$ rows and then also one of the $M-1$ remaining ones. We shall denote these minors by $F_i(z_1, \ldots, z_{2M})$, $i = 1, \cdots, M-1$, where $z_j \equiv \alpha_j$ and $z_{j+M} \equiv \alpha_j^*$ $(i = 1, \ldots, M)$ will be taken as $2(M-1)$ independent variables ($z_1 = z_{M+1} \equiv 1$). Again, this will only imply that when we now set

$$F_i(z_1, \ldots, z_{2M}) = 0, \tag{37}$$

for $i = 1, \cdots, M-1$, some of the solutions we find do not correspond to product vectors, although all the $|e_i, f_i\rangle$ we look for are among the solutions of (37).

We have $2(M-1)$ variables z_i and the same number $2(M-1)$ of polynomial equations for them, $M-1$ coming from the minors $F_i(z_1, z_{2M}) = 0$ and the remaining $M-1$ from its complex conjugation, which are inequivalent to the first ones as the variables are mapped according to $z_i \leftrightarrow z_{i+M}$, $i = 1, \cdots, M$, under complex conjugation.

No theorem exists for complex polynomials $P(\vec{\alpha}, \vec{\alpha}^*)$ which allows us to know the number of roots they have. However, in a *generic* case, namely when $P(\vec{\alpha}, \vec{\alpha}^*)$ is not proportional to its complex conjugate, we can prove that only a finite number of solutions exist. In [20] a method to find such roots was developed for polynomials depending on one α and its complex conjugate. Accordingly, from $P(\alpha, \alpha^*)$ another polynomial $Q(\alpha)$ containing all the roots of P was obtained. Such a method admits a generalization to the present case, which we shall discuss later on by means of an example when analyzing states of a 3×3 system. As already mentioned, we were not able to determine when a density matrix ϱ will lead to a set of *non-generic* polynomials. However, we expect this to be rarely the case. In what follows we will assume that the polynomials derived from ϱ are *generic*, and that therefore there is only a finite number of product vectors that can appear in (1).

C. Separability criterion.

When the number of solutions of equation (33) is finite, we can formulate a necessary and sufficient separability condition which follows from the following general theorem:

Theorem 2 (see also [8]) **.-** A state ϱ of rank $r(\varrho)$ is separable iff it can be written as a convex combination of at most $\min\{r(\varrho)^2, r(\varrho^{T_A})^2\}$ *linearly independent* projectors $|e_i, f_i\rangle\langle e_i, f_i|$ onto product vectors.

Proof.- The inverse implication is obvious. For the direct implication we will assume, without loss of generality, that $r(\varrho) \leq r(\varrho^{T_A})$. Caratheodoris' theorem tells us then that ϱ can be expressed as a convex combination of $r(\varrho)^2$ product projectors,

$$\varrho = \sum_{i=1}^{r(\varrho)^2} p_i |e_i, f_i\rangle\langle e_i, f_i|. \tag{38}$$

Suppose these projectors are not linearly independent. This means we can find $\sum_i c_i |e_i, f_i\rangle\langle e_i, f_i| = 0$ with at least some non-vanishing $c_i \in \mathcal{R}$. Set $\lambda \equiv \min\{p_i/c_i\}$. Then the decomposition

$$\varrho = \sum_{i=1}^{r(\varrho)^2} (p_i - \lambda c_i) |e_i, f_i\rangle\langle e_i, f_i|, \tag{39}$$

corresponds also to a convex combination of the previous projectors $|e_i, f_i\rangle\langle e_i, f_i|$, but with at least one of the terms having vanishing weight. Now, if the remaining projectors do not form yet a linearly independent set, we can repeat the same procedure and get rid of another product projector. This can be iterated until expressing ϱ as a convex combination of linearly independent product projectors. □

Consequently, once we obtain all product vectors $|e_i, f_i\rangle \in R(\varrho)$ such that $|e_i^*, f_i\rangle \in R(\varrho^{T_A})$, $i = 1, \cdots, L < \infty$, we can find out whether ϱ is separable by proceeding as follows:

- We build all possible maximal subsets of linearly independent projectors $|e_i, f_i\rangle\langle e_i, f_i|$ (with at least $L_0 \equiv \max\{r(\varrho), r(\varrho^{T_A})\}$ elements). Notice that there is only a finite number of subsets.

- For each of these subsets we express ϱ as a linear combination of projectors in the subset.

- If this is possible, then we have to see whether the coefficients of the linear combination are all positive.

We immediately have:

Separability criterion.- ϱ is separable iff all coefficients are non-negative in (at least) one of the linear combinations described above.

D. Numerical methods.

We notice that for a ϱ with just a finite, but large number L of eligible product vectors it may be impractical to construct all possible subsets of linearly independent product projectors, as described above. In this case the linear programming theory [28] has developed various methods to try to find out a solution to whether ϱ can be expressed as a linear combination, with positive weights, of the over complete but finite set of projectors $|e_i, f_i\rangle\langle e_i, f_i|$. We propose, however, to use for this aim the best separable approximation (BSA) method, developed by us in Ref. [16]. It has nice physical analogies also for non-separable states, providing the expansion

$$\varrho = \varrho_s + (1-\lambda)\delta\varrho,$$

where $\varrho_s = \sum_i \Lambda_i P_i$ is a separable state, $\lambda = \sum_i \Lambda_i$ is maximal, and finally $\delta\varrho$ is a state that does not have any product vector in its range. The paper [16] describes an efficient algorithm for finding such expansion, by optimizing each of the Λ_i individually, and each of the pairs Λ_i, Λ_j with respect to $\Lambda_i + \Lambda_j$. For the purpose of checking if a given matrix is separable, the BSA method of Ref. [16] is sufficient; in the context of the present paper it is interesting to introduce here a generalization of the results of [16] to the PPT states [29]:

Lemma 7.- Let ϱ be a PPT state. For a given set of $P_i = |e_i, f_i\rangle\langle e_i, f_i|$, such that the product vectors $|e_i, f_i\rangle \in R(\delta\varrho)$, such that $|e_i^*, f_i\rangle \in R(\delta\varrho^{T_A})$, there exists the best separable approximation of ϱ, in the form

$$\varrho = \varrho_s + (1-\lambda)\delta\varrho,$$

where $\varrho_s = \sum_i \Lambda_i P_i$ is a separable state, $\lambda = \sum_i \Lambda_i$ is maximal, and finally both $\delta\varrho \geq 0$, and $\delta\varrho^{T_A} \geq 0$. Moreover, there does not exist a product vector $|e, f\rangle \in R(\delta\varrho)$, such that $|e^*, f\rangle \in R(\delta\varrho^{T_A})$.

The proof of the above lemma is the same as the proof in Ref. [16]. Similarly, one can find an efficient algorithm for finding the BSA, by requiring that:

- All Λ_i should be maximal, i.e.

$$\Lambda_i = \min\left(\langle e_i, f_i|(\rho - \sum_{j\neq i}\Lambda_j P_j)^{-1}|e_i, f_i\rangle^{-1}, \right.$$
$$\left. \langle e_i^*, f_i|(\rho^{T_A} - \sum_{j\neq i}\Lambda_j P_j^{T_A})^{-1}|e_i^*, f_i\rangle^{-1}\right). \quad (40)$$

- All pairs of Λ_i, Λ_j should be maximized with respect to $\Lambda_i + \Lambda_j$. This requirement can also be expressed in an analytical form for Λ's, which will be presented elsewhere [31].

E. Example: 3×3 system.

We end this section by describing with an example in a 3×3 system how to estimate the number L of eligible product vectors. This example illustrates how to generalize to several independent α's the method developed in [20].

Suppose $r(\varrho) \leq 4$ and $r(\varrho^{T_A}) \leq 9$. For $r(\varrho) = 4$ and $r(\varrho^{T_A}) = 9$ (least favorable case) we have that the matrix A reads

$$A = \begin{bmatrix} \langle k_1^1| + \alpha_2\langle k_1^2| + \alpha_3\langle k_1^3| \\ \langle k_2^1| + \alpha_2\langle k_2^2| + \alpha_3\langle k_2^3| \\ \langle k_3^1| + \alpha_2\langle k_3^2| + \alpha_3\langle k_3^3| \\ \langle k_4^1| + \alpha_2\langle k_4^2| + \alpha_3\langle k_4^3| \\ \langle k_5^1| + \alpha_2\langle k_5^2| + \alpha_3\langle k_5^3| \end{bmatrix}, \quad (41)$$

so that after constructing the 3×3 submatrices $A_{1,2,3}$ by taking the first two rows of A and one of the remaining rows at a time, we obtain three 3-rd order equations for α_1 and α_2:

$$F_1 = \det M_1 \equiv \sum_{k=0}^{3} \alpha_2^k P_3^k(\alpha_3) = 0, \quad (42)$$

$$F_2 = \det M_2 \equiv \sum_{k=0}^{3} \alpha_2^k Q_3^k(\alpha_3) = 0, \quad (43)$$

$$F_3 = \det M_3 = 0, \quad (44)$$

where $P_s(x)$ denotes a s-th order polynomial in x. By only using equations (42) and (43) we can obtain two quadratic equations in α_2 as follows: on the one hand we multiply (42) by $Q_3^3(\alpha_3)$, (43) by $P_3^3(\alpha_3)$, and then subtract them, leading to

$$\sum_{k=0}^{2} \alpha_2^k R_6^k(\alpha_3) = 0; \quad (45)$$

on the other hand we multiply (42) by $Q_3^0(\alpha_3)$, (43) by $P_3^0(\alpha_3)$, again subtract them, and after dividing by α_2 we obtain

$$\sum_{k=0}^{2} \alpha_2^k S_6^k(\alpha_3) = 0. \quad (46)$$

Finally, applying the same trick but now to equations (45) and (46), we obtain two linear equations for α_2, from which a unique 18-th order equation for α_3 follows. Therefore there are at most 18 different values of α_3 which in principle could lead to an eligible product vector. For each such values one should now still solve the 3 3rd order equations (42-44) for α_2, and see which solutions survive, if any [2] . Finally, for those triads $[1, \alpha_2, \alpha_3]$ which indeed fulfill (42-44) we can diagonalize A and find the corresponding Bob's local vector $|f\rangle$ in the kernel of A. We have obtained, thus, $L \leq 18$.

Before going into the conclusions we shall discuss briefly the question of the relative size of $r(\varrho)$ and $r(\varrho^{T_A})$. It is natural to expect that this difference is not too big. However some naive intuitions must be abandoned (see [30]). Here we shall make the simple observation:

Observation .- Let ϱ be a PPT state. If kernel of ϱ contains the range of some PPT state σ, then the kernel of ϱ^{T_A} contains the range of σ^{T_A}, so that $r(\varrho^{T_A}) \leq MN - r(\sigma^{T_A})$.

The above observation about rank of ϱ follows easily from the fact that $\mathrm{Tr}(AB) = \mathrm{Tr}(A^{T_A} B^{T_A})$. Note that σ can be a separable state. In particular, if the kernel of ϱ contains any system of n orthogonal product vectors (in particular UPB set [17]) then $r(\varrho^{T_A})$ can not exceed the value of $MN - n$. The same holds if σ from our observation is PPT bound entangled state defined as a UPB complement [17]. The rank of the latter does not change under partial transpose, so again $r(\varrho^{T_A})$ can not exceed the value of $MN - r(\sigma)$. It can be also extended in other direction: taking σ as a nontrivial PPT invariant state. Apart from all σ's being complements of real UPB's, there is an other nontrivial class (provided in [32]) of $N \times N$ states of that kind all having $r(\sigma) = \frac{N(N-1)}{2} + 1$. From the above discussion and the Theorem 1 we immediately know, for example, that for all the 3×3 PPT entangled states with the kernel containing UPB complement both ranks: $r(\varrho^{T_2})$ and $r(\varrho^{T_2})$ must amount to either 4 or 5 so they cannot differ much from each other.

V. CONCLUSIONS

We have presented in this paper a relatively complete list of separability criteria for density matrices of low rank. There are several problems, however, which remain open and are worth further studies:

- In our analysis of the kernels of ϱ and ϱ^{T_A} we have essentially used only those of their properties that are consequences of the dimensionality. On the other hand, it is expectable that both kernels are structurally related through the partial transpose operation. It would be important to investigate such relations, since it would probably automatically put much more stringent restrictions on the existence of separable matrices of low rank.

- All of the results of this paper can be generalized to the case of multipartite systems, and in particular 3 partite systems. We have already obtained several results, but we leave a detailed and complete discussion of this problem to a separate publication. Let us just mention here that according to our studies: i) there are no rank N PPT entangled states for $N \times N \times N$ systems; ii) In $2 \times 2 \times 2$ spaces PPT states of rank 4 are separable with respect to 2×4 space of Alice and joint space of Bob and Charles, and posses a unique decomposition into a sum of 4 projectors onto product vectors in 2×4 space; they are fully separable iff those 4 product vectors are at the same time product vectors in the sense of $2 \times 2 \times 2$; iii) In $2 \times 2 \times 2$ spaces generic PPT states with $r(\varrho) + r(\varrho^{T_A}) + r(\varrho^{T_B}) + r(\varrho^{T_C}) \leq 4 \times 8 - 2 \times 2 + 1 = 29$ have a finite number of product vectors in their range, such that the partial conjugates of those product vectors are in the corresponding ranges of partial transposes.

This work has been supported by Deutsche Forshungsgemeinschaft (SFB 407 and Schwerpunkt "Quanteninformationsverarbeitung"), the Österreichisher Fonds zur Fẗderung der wissenschaftlichen Forschung (SFB P11), the European TMR network ERB-FMRX-CT96-0087, and the Institute for Quantum Information Gmbh. J. I. C. thanks the University of Hannover for hospitality. P. H. acknowledges the grant from Deutscher Akademisher Austauschdienst. We thank S. Karnas, A. Sanpera, J. Smolin, B. Terhal for fruitful discussions. We thank J. Werner for indicating to us relations to linear programming theory.

[2] Notice that for a given α_3 in principle we could find $0, 1, 2$ or 3 valid values of α_2. For simplicity we assume in the final estimation of the number L of eligible product vectors that to each solution α_3 there corresponds at most one valid α_2.

* E-mail address: pawel@mifgate.pg.gda.pl
** E-mail address: lewen@itp.uni-hannover.de
*** E-mail address: Guifre.Vidal@uibk.ac.at
**** E-mail address: Ignacio.Cirac@uibk.ac.at

[1] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47** (1935) 777.

[2] E. Schrödinger, Proc. Cambridge Philos. Soc. **31** 555 (1935).
[3] A. Ekert, Phys. Rev. Lett. 67 (1991) 661. C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. 69 (1992) 2881. C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[4] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996); D. Deutsch, A. Ekert, R. Jozsa, Ch. Macchiavello, S. Popescu and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[5] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. Lett. **78** (1997) 574.
[6] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[7] R. Werner, Phys. Rev. A **40** (1989) 4277.
[8] P. Horodecki Phys. Lett. A **232** (1997) 333.
[9] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **230**, 377 (1996).
[10] A. Peres Phys. Rev. Lett. **76** 1413 (1996),
[11] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Lett. A **223**, 1 (1996);
[12] S. L. Woronowicz, Rep. Math. Phys., **10** (1976) 165.
[13] M. D. Choi, Proc. Sympos. Pure. Math. **38** (1982) 583
[14] K. Życzkowski, P. Horodecki, A. Sanpera and M. Lewenstein, Phys. Rev. A **58**, 883 (1998).
[15] G. Vidal and R. Tarrach, Phys. Rev. A **59**, 141 (1999). See also S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu and R. Schack, Phys. Rev. Lett. 83 1054 (1999).
[16] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261, (1998).
[17] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin and B. M. Terhal, Phys. Rev. Lett. **83**, 3081 (1999); D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin and B. M. Terhal, quant-ph/9908070; C. H. Bennett, D. P. DiVincenzo, Ch. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin and W. K. Wootters, quant-ph/9804053; see also R. Horodecki, M. Horodecki, and P. Horodecki, quant-ph/9811004.
[18] B. Terhal, quant-ph/9810091.
[19] A. Sanpera, R. Tarrach, and G. Vidal, Phys. Rev. A **58**, 826 (1998).
[20] B. Kraus, J. I. Cirac, S. Karnas and M. Lewenstein quant-ph/9912010; see also M. Lewenstein, J. I. Cirac and S. Karnas, /quant-ph9903012.
[21] D. Bruß and A. Peres, quant-ph/9911056.
[22] Though the problem was reduced to the one parameter question about one parameter Werner states [33] and recent results strongly suggest the that NPT BE states exist [W. Dür, I. Cirac, M. Lewenstein and D. Bruß, quant-ph/9910022], [D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. Terhal and A. Thapliyal, quant-ph/9910026]. The complete solution seems to be by no means trivial. It is only known that there is no PPT BE states in the case $2 \times N$ [20].
[23] P. Horodecki, M. Horodecki and R. Horodecki. Phys. Rev. Lett. **82**, 1056 (1999).
[24] P. Horodecki, M. Horodecki and R. Horodecki, quant-ph/9904092, J. Mod. Opt. (in press).
[25] V. Vedral, Phys. Lett. A **262** (1999) 121.
[26] P. Horodecki, J. A. Smolin, B. M. Terhal and A. V. Thapliyal, quant-ph/9910122.
[27] Let $|\Psi_f\rangle \equiv \begin{bmatrix} |f\rangle \\ -F|f\rangle \end{bmatrix}$ and $M \equiv \begin{bmatrix} E & F^\dagger \\ F & I \end{bmatrix} \geq 0$, where $|f\rangle \in \mathcal{C}^N$ and E, F, I are operators on $\mathcal{C}^N$. Then $\forall |f\rangle$ we have $\langle \Psi_f | M | \Psi_f \rangle = \langle f | E - FF^\dagger | f \rangle \geq 0$.
[28] D. Luenberger, "Introduction to Linear and Nonlinear Programming", (Addison-Wesley, Massachusets, 1984); D. Gale, "The Theory of Linear Economic Models", (MC Graw-Hill, New York, 1960).
[29] The generalization of this lemma to the case of continuous indices as well as its application will be considered elsewhere (P. Horodecki, M. Lewenstein, M. Horodecki, R. Horodecki, in preparation).
[30] D. P. DiVincenzo, B. M. Terhal and A. V. Taphliyal, quant-ph/9904005.
[31] S. Karnas and M. Lewenstein, to be published.
[32] P. Horodecki and M. Lewenstein, quant-ph/0001035.
[33] M. Horodecki and P. Horodecki, Phys. Rev. A **52** (1999) 4206.